CLAIMS

1. A secure method for sending an encrypted command from a remote keyless entry device to a receiver in a motor vehicle comprising the steps of:

defining a key generating key within the remote keyless entry device;

generating a working key from the key generating key;

transmitting the working key from the remote keyless entry device to the receiver during a training session without transmitting the key generating key; and

transmitting a message encrypted with the working key from the remote keyless entry device to the receiver.

2. The secure method of claim 1 wherein the step of generating a working key comprises the step of using an encryption algorithm to combine an output of an incrementing mechanism with the key generating key.

3. The secure method of claim 2 wherein the incrementing mechanism comprises a first counter and wherein the method further comprises the steps of:

incrementing the first counter to provide an incremented output of the first counter; and

generating a new working key each time the remote keyless entry device enters a training session.

4. The secure method of claim 3 further comprising the steps of:

incrementing a second counter in the remote keyless entry device to provide a second incremented output each time a message is transmitted from the remote keyless entry device and

synchronizing a third counter in the motor vehicle to provide a third incremented output each time a message transmitted by the remote keyless entry device is received by the receiver and verified to be a valid message.

5. The secure method of claim 4 wherein the step of transmitting a message comprises the step of transmitting a message comprising an encrypted version of the second incremented output.

6. The secure method of claim 5 further comprising the steps of:

decrypting the message at the receiver using the working key; and

verifying the validity of the message using the third incremental output.

7. The secure method of claim 6 wherein the step of verifying comprises the step of comparing a third incremented output to the second incremented output.

8. The secure method of claim 2 wherein the step of using an encryption algorithm comprises the step of using a block encryption algorithm to combine the output of the incrementing mechanism with the key generating key.

9. The secure method of claim 1 wherein the step of transmitting a message comprises the step of transmitting a message comprising a command and an identifier.

10. A secure remote keyless entry system for a motor vehicle comprising:

a remote keyless entry device comprising a key generating encryption key configured to generate a working key and a transmitter configured to transmit a ciphertext command encrypted with the working key without transmitting the key generating key; and

a receiver positioned in the motor vehicle and configured to receive and decrypt the ciphertext command encrypted with the working key.

11. The secure remote keyless entry system of claim 10 wherein the remote keyless entry device further comprises encryption circuitry and the receiver comprises decryption circuitry.

12. The secure remote keyless entry system of claim 11 further comprising a first incrementable counter configured to provide an incrementable output and wherein the incrementable output, the working key, and a plain text command comprise inputs to the encryption circuitry.

13. The secure remote keyless entry system of claim 12 further comprising a second incrementable counter configured to provide a second incrementable output for verifying the validity of the received ciphertext command.

14. A remote keyless entry device for a motor vehicle comprising:

a key generating key stored in and never transmitted from the remote keyless entry device;

a non volatile counter configured to provide an incrementable output;

an encryption circuit coupled to receive the key generating key and the output of the non volatile counter and configured to generate a working key; and

a transmitter configured to send a command message encrypted with the working key.

15. The remote keyless entry device of claim 14 wherein the transmitter can be further configured in a training mode for transmitting the working key to a receiver in a motor vehicle.

16. The remote keyless entry device of claim 14 further comprising a second counter having an output, a device identifier, and a plurality of command selections, and wherein the transmitter comprises a transmitter configured to transmit a command message comprising an encrypted version of the output, the device identifier, and one of the plurality of command selections.

17. A method for sending an encrypted command from a remote keyless entry device comprising a key generating key that is never transmitted from the remote keyless entry device, an incrementable first counter, encryption circuitry, a second incrementable counter, a device identifier, a plurality of command selections, and a transmitter to a receiver in a motor vehicle comprising decryption circuitry and an incrementable third counter, the method comprising the steps of:

generating a working key from the key generating key and an output of the incrementable first counter using an encryption algorithm;

transmitting the working key from the remote keyless entry device to the receiver during a training session;

transmitting a command message to the receiver, the command message comprising an output of the second incrementable counter, the device identifier, and one of the plurality of command selections at least a portion of which are encrypted by the encryption circuitry using the working key;

receiving the command message at the receiver;

decrypting the command message by the decryption circuitry using the working key; and

verifying the validity of the command message using an output of the incrementable third counter.

18. The method of claim 17 further comprising the steps of:

incrementing the second incrementable counter each time the transmitter transmits a command message; and

synchronizing the incrementable third counter to the second incrementable counter each time the receiver receives a valid command message.

19. The method of claim 17 wherein the step of generating a working key comprises the step of generating a working key from the key generating key and an output of the incrementable first counter using an encryption algorithm.

20. The method of claim 19 wherein the step of generating a working key comprises the step of generating a working key from the key generating key and an output of the incrementable first counter using a block encryption algorithm.

21. A rolling code remote keyless entry system for a motor vehicle comprising:

a remote keyless entry transmitter;

a key generating key in the remote keyless entry transmitter, the key generating key never transmitted from the remote keyless entry transmitter;

an incrementable counter in the remote keyless entry transmitter having an output; and

a mechanism in the remote keyless entry transmitter for generating a working key from the key generating key and the output.

22. A rolling code remote keyless entry system for a motor vehicle comprising:

a key generating key provided in a remote keyless entry device and never transmitted from the remote keyless entry device;

a number generator configured to generate a number for use as a working key, the number comprising a number selected from the group consisting of random numbers and pseudorandom numbers and based on the key generating key;

a transmitter configured to transmit the working key to a motor vehicle during a training session.